SZECSKÓ ENIKŐ*

Az információs szabadságjogok érvényesülése a rendvédelemben

I. Bevezető gondolatok[1]

A felgyorsult információtechnológiai fejlődés és ennek hatására az adatok megszerzésének, kezelésének és tárolásának kibővült lehetőségei, a személyes adatok megfelelő védelmének jogi szabályozását napjaink fontos kérdésévé tette. A technikai fejlődés, az infokommunikációs rendszerek fejlesztése sokkal gyorsabb ütemű, mint az ezekre reflektáló jogszabályi változások, így a szabályozásnak rendkívül dinamikusan kell alkalmazkodjon a tudományos előrelépések mértékéhez.

Az információs szabadságjogok két fő területe a személyes adatok védelme és a közérdekű, illetve a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jog, amelyeket Magyarország Alaptörvénye a VI. cikk 3) bekezdésében deklarálja: „[m]indenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez."[2] Az információs önrendelkezési jog és az információszabadság törvényi szabályozása hazánkban nem tekint vissza hosszú múltra. Habár a rendszerváltás után, 1989-től alkotmányos jogként megfogalmazódott, elsőként csak a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény szabályozta ezt a kérdéskört. Ezt megelőzően is találhatunk azonban adatvédelmi jellegű megállapításokat, hiszen az Alkotmánybíróság már a 15/1991. (IV. 13.) határozatában leszögezte: „[m]indenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad."[3] Egy mindenkit megillető alapjogként értelmezhető tehát az adatvédelem, ezzel szemben nem korlátozhatatlan, hiszen „más alapvető jog érvényesülése vagy alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan"[4] korlátozható a joggyakorlás lehetősége.

---

* SZTE ÁJTK

1 A mű alapját a szerzőnek a Nemzeti Adatvédelmi és Információszabadság Hatóság joghallgatóknak kiírt pályázatán bemutatott dolgozata jelentette. l. SZECSKÓ ENIKŐ: *Adatvédelem a nemzetbiztonsági szolgálatok tevékenységének körében.* 2017.

2 Alaptörvény, VI. cikk, (3) bekezdés.

3 15/1991. (IV. 13.) AB határozat, ABH 1991. 40, 42.

4 Alaptörvény. I. cikk, (3) bekezdés.

A bűnüldöző szervek és a nemzetbiztonsági szolgálatok tevékenysége során előforduló leplezett eszközök használata és a titkos információgyűjtés kivitelezése is meg kell feleljen az alkotmányos alapelvi szükségességi-arányossági mércének ahhoz, hogy a törvényesség határai között helyezkedjen el. Rendvédelmi szervek alatt a dolgozatban a nemzetbiztonsági szolgálatok és Magyar Rendőrség együttesen értendő, hiszen a rendvédelem kifejezés nem a rendészet szinonimája, hanem annál tágabb[5] fogalom, ide tartozik minden olyan tevékenység, amelynek célja a „rend megóvása a támadásoktól, erőszakos cselekményektől, veszélyektől."[6]

A dolgozat első részében kifejezetten a nemzetbiztonsági szervek[7] titkos információgyűjtési tevékenységeinek vonatkozásában, a jelenlegi adatvédelmi szabályozások állampolgárokra gyakorolt védelmi mechanizmusát vizsgálom. A korlátozott terjedelem miatt, a Magyar Rendőrség és az egyéb feljogosított szervek leplezett eszközökkel történő eljárásainak áttekintése nem képezi a dolgozat tárgyát.

A második részben a hazai információszabadsági gyakorlatot a Magyar Rendőrség, illetve az öt hazai nemzetbiztonsági szerv közötti összehasonlító elemzésben mutatom be. Az összehasonlítás alapját az általam benyújtott 28 db közérdekű adatigénylés (I. melléklet) adta, amelyeknek összesített eredménye (II. melléklet) az V. fejezetben bemutatott hipotézisemet alátámasztja. Végezetül a bemutatott kérdéskörök kapcsán de lege ferenda javaslatot is megfogalmaztam, mind az adatvédelemi témakörben, mind az információszabadság gyakorlati megvalósulásának javítása érdekében.

II. Az adatvédelem általános elvei[8]

1. Célhoz kötött adatkezelés elve

A célhoz kötött adatkezelés elve két főbb elemből épül fel, ezek a cél meghatározottsága és a megszerzett adatnak, az előzetes céllal való összeegyeztethető felhasználása[9]. A cél meghatározottsága azt jelenti, hogy a személyes adatok csak egyértelmű, meghatározott és törvényes célból gyűjthetőek, jog gyakorlása vagy kötelezettség teljesítése érdeké-

---

[5] ERNYES MIHÁLY: *Rendvédelem, rendvédelem-történet (fogalmi és tartalmi megközelítés)*. Rendvédelem-történeti Füzetek 2015/25(43–46). 16. p.

[6] MEZEY BARNA: *Közigazgatási jog – rendvédelmi jog.* 33. p. In.: Boda József (szerk.): *A* magyar polgári rendvédelem a XIX-XX. században. A magyar büntetés-végrehajtás, csendőrség, határőrség, koronaőrség, *rendőrség, vám- és pénzügyőrség.* Belügyminisztérium Nemzetközi Oktatási Központ – Szemere Bertalan Magyar Rendvédelem-történeti Alapítvány. Budapest, 2004

[7] A hazai nemzetbiztonsági szolgálatok a következők: az Információs Hivatal, az Alkotmányvédelmi Hivatal, a Katonai Nemzetbiztonsági Szolgálat, a Nemzetbiztonsági Szakszolgálat, valamint a Terrorelhárítási Információs és Bűnügyi Elemző Központ.

[8] A személyes adatok védelme esetén, a hazai általános törvényi szabályozás keretét a 2011. évi információs önrendelkezési jogról és az információszabadságról szóló CXII. törvény (a továbbiakban: Infotv.) adja. Európai Uniós szinten az általános adatvédelmi előírásokat az Európai Parlament és a Tanács 2016/679 számú rendelete, míg kifejezetten a bűncselekményekre vonatkozó adatok kezelésének előírásait az Európai Parlament és a Tanács (EU) 2016/680 Irányelve szabályozza.

[9] 15/1991. (IV. 13.) AB határozat.

ben. Az adatok felvételét a cél rögzítése meg kell előzze, valamint a meghatározottságnak az adatkezelés minden szakaszában jelen kell lennie.[10]

Az érintettek[11]hozzájárulásán alapuló adatkezelés[12] során, az összeegyeztethető felhasználás az adatalany által is ismert cél megvalósulásáig tart. Amikor az adatkezelés jogszabályi felhatalmazáson alapul, akkor az érintett tudtán kívül is történhet, tehát az adatalanynak nincs lehetősége az adatai célhoz kötött és az ezzel összeegyeztethető kezelés ellenőrzésére. Ezekben az esetekben rendkívül fontos a személyes adatok kezelésével és felhasználásával kapcsolatban a pontos, mindenre kiterjedő jogszabályi háttér, a jogsértések és az adatvédelemi incidensek elkerülése végett.

1.1. Szükségesség követelménye

A szükségesség, vagy más néven az adatminimalizálás elve alatt az értendő, hogy csak olyan és annyi személyes adat kezelhető, amelyek beszerzése az előre rögzített cél eléréséhez nem mellőzhető, nélkülözhetetlen és ezen felül alkalmas is a feladat teljesítéséhez. A célhoz kötött adatkezelés a szükségesség előfeltétele, hiszen a cél határozza meg a beszerzendő adatok mértékét. A 2/1990 (II. 18.) AB határozat alapján az adatkezelés alapjogsértő, ha eleve alkalmatlan a cél elérésére, vagy ha kevesebb adattal is elérhető a kitűzött cél, így ebben az esetben a többlet adatkezelés mértéke lesz jogsértő. Jogszerűtlen az olyan adatok kezelése, amelyek nem alkalmasak vagy nem elengedhetetlenek az adatkezelés céljának eléréséhez.

1.2. A készletező adatkezelés tilalma

A célhoz kötött adatkezelés elvéből következik a készletező adatkezelés tilalma is, ami alapján a személyes adatok gyűjtése és kezelése csak „a cél megvalósulásához szükséges mértékben és ideig kezelhető".[13] Tehát a meghatározott cél megvalósítása után, vagy az azt meghaladó mérték esetén, a személyes adatok kezelése, még az érintett hozzájárulása mellett sem tekinthetők jogszerűnek,[14] az ilyen adatot minden adatkezelő köteles törölni a rendszeréből.

Amennyiben nem az érintett, hanem az adatok kezelőjének szemszögéből vizsgáljuk ezt a tilalmat, akkor azt láthatjuk, hogy egy rendkívül kényelmetlen és nem gazdaságos szabályozás, hiszen az adatok folyamatos tárolása sokkal kevesebb anyagi és emberi erőforrást igényelne, mint ugyanabból a célból, egy későbbi adatgyűjtés újbóli kivitelezése. Ezzel szemben elmondható, hogy a személyes adatok védelmének törvényi szabá-

[10] Lásd: A 29. cikk szerinti munkacsoport 03/2013. számú, a célhoz kötöttségről szóló véleménye.

[11] Infotv. 3. § (1) „*érintett: bármely információ alapján azonosított vagy azonosítható természetes személy*."

[12] Infotv. 3. § (10) „*adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése*."

[13] Infotv. 4.§ (2).

[14] JÓRI ANDRÁS–SOÓS ANDREA KLÁRA: *Adatvédelmi jog.* HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2016. 152. p.

lyozása nem az adatkezelők és adatfeldolgozók kényelmét és gazdasági érdekeit tartja szem előtt, hanem az érintett alkotmányos jogait és magánszférájának védelmét.

2. Az adatkezelés jogalapja

A személyes adatok kezelése az érintett hozzájárulásán[15] vagy jogszabály közérdekű cél teljesítéséből történő előírásán alapulhat. Az érintett hozzájárulása lehet szóbeli, írásbeli[16] vagy ráutaló magatartással kifejtett, de minden esetben megfelelő tájékoztatás kell, hogy megelőzze. A jogszabályon alapuló, kötelező adatkezeléshez nem szükséges az érintett hozzájárulása, sőt, kifejezett tiltakozása ellenére is kezelhetőek az adatai. Az Infotv. a régi Adatvédelmi törvényhez[17] képest két új, másodlagos jogalapot is teremtett. Amennyiben az adatkezelőre jogi kötelezettség teljesítése írja elő a személyes adatok kezelését, illetve ha harmadik személy olyan érdeke fűződik az adatok megismeréséhez, amely arányos az adatok védelmének korlátozásával, szintén megteremti a jogalapot. A jogi kötelezettség teljesítése során történő adatkezelés, az érintett hozzájárulása vagy törvényi felhatalmazás nélkül is jogszerű. A nemzetbiztonsági célú titkos információgyűjtési tevékenységére vonatkozó törvényi felhatalmazást a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) 39. § (1) bekezdés e) pontja szolgáltatja.

3. Arányosság

A személyes adatok nem megfelelő kezelése esetén az Alaptörvényben lefektetett információs önrendelkezési jog gyakorlása sérülhet, kiváltképpen a titkos információgyűjtésből származó adatok esetében. Ahhoz, hogy az adatkezelő eljárása a jog talaján nyugodjon, szükséges, hogy az intézkedés a legkisebb beavatkozást jelentse az érintett magánszférájába. Az Nbtv. a 31. § (6) bekezdése az arányosságot így fogalmazza meg: „több lehetséges és alkalmas intézkedés, illetőleg kényszerítő eszköz közül azt kell választani, amely az eredményesség biztosítása mellett az intézkedéssel érintettre a legkisebb korlátozással, sérüléssel vagy károkozással jár.”[18] Az arányosság fogalmi elemei az adatkezelés céljának és a személyes adatok védelmében bekövetkezett sérelem mértékének arányossága, valamint a cél érdekében, a legenyhébb sérelemmel járó és alkalmas eszköznek az igénybe vétele.[19]

---

[15] Infotv. 3. § (7) „*hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez*.”

[16] Különleges adatot (Infotv. 3. § 3.) csak írásbeli hozzájárulás alapján lehet kezelni.

[17] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (hatályát vesztette: 2012. január 1.)

[18] Nbtv. 31. § (6)

[19] RÉVÉSZ BÉLA**:** *Források a titkosszolgálatok politológiai tanulmányozásához.* JATE Press Kiadó. Szeged, 2010. 121. p.

4. Adatbiztonság követelménye

Az adatbiztonság[20] az elektronikus rendszerekben tárolt adatokkal kapcsolatos olyan előírás, amely alapján az adatkezelés teljes tartama alatt biztosítani kell az adatok sértetlenségét,[21] rendelkezésre állását[22] és bizalmas[23] kezelését. Ezek a feltételek nem csak a kezelt adatok kapcsán, hanem az adatkezelő rendszerrel összefüggésben is fennállnak[24]. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezésein alapuló információbiztonsági hatósági feladatot és biztonsági felügyeletet a nemzetbiztonsági szolgálatok[25] esetében kormányrendeletben megállapított feltételek szerint, egy, a szervezeten belül létrehozott ellenőrző szerv látja el. Kérdéses, hogy ilyen ellenőrzési feltételek mellett a titkos információgyűjtésből származó adatok nem megfelelő kezelése esetén, hogyan lehet megállapítani a személyi felelősségét, illetve a jogsértések megakadályozásának, biztonsági események[26] bekövetkezte esetén a megfelelő kivizsgálásnak milyen független, szervezeten kívüli lehetőségei vannak.

5. Osztott információs rendszerek követelménye

A személyes adatok kezelőjével szembeni követelmény, amely alapján az adatkezelő ugyanarról az érintettről, csak a számára szükséges, minimális mennyiségű személyes adathoz férhet hozzá. Az információs rendszerek osztottságának a célja, hogy az adatkezelő ne legyen képes az érintett személyiségi profiljának a felállítására azáltal, hogy több, eltérő típusú személyes adat is koncentrálódik a kezelési körében.[27] Az adatvédelemnek nem célja, hanem hasznos következménye az a tény, hogy az adatok koncentrációjának csökkentésével, az ezeket felhasználó állami szervek állampolgárokra gyakorolt hatalmi befolyása is redukálódik, így végső soron az állami hatalom koncentrációját is csökkenti.[28]

---

[20] Az adatbiztonságot a német Alkotmánybíróság (Bundesverfassungsgericht) az általános személyiségi jogból levezetve, külön alapjogként határozta meg. Lásd: 1 BvR 370/07. 2008. február 27.

[21] 2013. évi L. törvény 1. § (39) „*sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek (…)*."

[22] 2013. évi L. törvény 1. § (38) „*rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek."*

[23] *2013. évi L. törvény 1. § (8) „bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról*."

[24] Az adatbiztonság követelményeiről az 1998. évi az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló VI. törvény 7. cikk rendelkezik.

[25] A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény 1. § (2) h) pontja alapján a rendvédelmi szervek és a Katonai Nemzetbiztonsági Szolgálat is központi államigazgatási szervnek minősül, így a 2013. évi L. törvény hatálya alá tartoznak.

[26] 2013. évi L. tv. 1. § (9) „*biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül*;"

[27] 2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről, 2. § (1)

[28] SZABÓ MÁTÉ DÁNIEL: *Hogyan érdemes gondolkodni adatvédelemről és információszabadságról?* Fundamentum. 2007/1. 124. p.

III. A titkos információgyűjtés adatvédelmi kérdései

A nemzetbiztonsági szolgálatok alapvető feladata az Alaptörvény 46. cikk (3) bekezdése alapján „Magyarország függetlenségének és törvényes rendjének védelme, nemzetbiztonsági érdekeinek érvényesítése."[29]Arról, hogy e feladat megvalósítása milyen jogszabályi környezetben történjen, sarkalatos törvény, az Nbtv. gondoskodik.

A titkosszolgálatok esetében az alkotmányos kontrollt, a szervezetek speciális jellemzői és tevékenységi köre miatt nem a részletekbe menő nyilvános előírások és szabályozás jellemzi. A hírigények teljesítése érdekében végzett műveletek fő korlátját az Alaptörvényben is megjelenő szükségességi-arányossági teszt[30] jelenti. A 23/1990. (X. 31.) AB határozat alapján az egyén autonómiájának létezik egy érinthetetlen belső halmaza, amelyre nem terjedhet ki még az állam kényszerítő hatalma sem.[31] Ennek értelmében alapjogok korlátozása esetén – ilyen a titkos információgyűjtés és az ebből származó személyes adatok kezelése is, – alkotmánysértő az adott alapjog lényeges tartalmát elérő, korlátozó sérelem.[32]A nemzetbiztonsági érdekre való hivatkozás alapul szolgál a magánszféravédelem[33] általános szabályaitól való eltérő gyakorlatra, hiszen e szervek elsődleges feladata az ország szuverenitásának oltalma, az alkotmányos rendet sértő tevékenységek felismerése és megakadályozása, így végső soron az állam védelme.[34] Ebből kifolyólag, mivel egy elsődleges állami érdek ütközik egy korlátozható alapjoggal, a személyes adatok védelméhez való jog teljes érvényesítése csak a lényeges, érinthetetlen halmazon belül garantálható az állam részéről.

A nemzetbiztonsági szolgálatok alkotmányos működését garantálja, hogy mindhárom hatalmi ág részt vesz a működésében. A kormány szerepe a szolgálatok irányítása, míg a parlament feladata ennek ellenőrzése.[35] A bírói szerepvállalás a titkos információgyűjtés engedélyezésében és a külső törvényességi kontroll fenntartásában jelenik meg.[36]

[29] Alaptörvény, 46. cikk, (3)
[30] Alaptörvény, I. cikk, (3)
[31] 23/1990. (XI. 31.) AB határozat.
[32] 15/1995. (III. 13.) AB határozat.
[33] *„A magánszféra lényegi fogalmi eleme éppen az, hogy az érintett akarata ellenére mások oda (...) be se tekinthessenek. Ha a nem kívánt betekintés mégis megtörténik, akkor nemcsak önmagában a magánélethez való jog, hanem az emberi méltóság körébe tartozó egyéb jogosultsági elemek, mint pl. az önrendelkezési szabadság vagy a testi-személyi integritáshoz való jog is sérülhet."* 36/2005. (X. 5.) AB határozat, ABH 2005. 390, 400.
[34] SOLTI ISTVÁN: *A titkos információgyűjtés törvényessége.* Nemzetbiztonsági Szemle 2013/1(1). 5–18. pp.
[35] IZSA JENŐ–SZILÁGYI ZSOLT: *A nemzetbiztonsági szolgálatok parlamenti ellenőrzésének elvi és gyakorlati kérdései.* KBH Szakmai Szemle 2007/3. 5–30. pp.
[36] IZSA JENŐ: *Nemzetbiztonsági alapismeretek (A titkosszolgálatok működése) – Egyetemi jegyzet*, Zrínyi Miklós Nemzetvédelmi Egyetem, Kossuth Lajos Hadtudományi Kar, Biztonság- és Védelempolitikai Tanszék. Budapest, 2009. 8. p.

1. Kitekintés: A nyílt információgyűjtés[37]

A dolgozat elsődleges témája a titkos információgyűjtésből származó személyes adatok védelmének kérdéskörére fókuszál, de a nemzetbiztonsági szervek tevékenységének csak egy meghatározott hányadát[38] teszik ki az e forrásból származó adatok, ezért nem hagyható figyelmen kívül a nyílt információgyűjtésből származó személyes adatok kezelésének a vizsgálata sem.

Ha a nyílt információgyűjtés definícióját negatív tartalom alapján próbáljuk megfogalmazni, akkor minden információgyűjtő tevékenység, amely nem titkos információgyűjtésből származik, ebbe a körbe tartozik. Nyílt információgyűjtés során a hírigények teljesítése érdekében folytatott tevékenységek szükségszerűen kapcsolódnak a személyes adatokhoz való hozzáféréshez is. Ehhez leggyakrabban, de nem kizárólagosan, az Internet szolgáltatja az adatok beszerzési felületét. Azonban az a tény, hogy egy adott személynek a személyes adatai online, nyílt felületen hozzáférhetővé váljanak, nagy valószínűséggel feltételezi az adatok előzetes, nem megfelelő védelmét[39] az adatkezelő vagy az adatalany részéről. A nyílt információgyűjtés teljes mértékben meg kell feleljen a személyes adatok védelmére irányuló általános előírásoknak, tekintve hogy az Infotv. csak az érintett személyes célra történő adatkezelését veszi ki a törvény hatálya alól, ellenben ha nem nyílt, hanem titkos információgyűjtés kategóriájába esik a tevékenység, akkor az Nbtv. megfelelő rendelkezései[40] az irányadóak. További felmerülő probléma, hogy amennyiben egy nyílt forrású információgyűjtésből származó összesített adatcsoportot[41] a 2009. évi CLV. törvény alapján minősítési eljárás alá vonnak, attól még az adatok eredeti forrása ugyanúgy elérhető a civil, de hozzáértő publikum számára, míg a közel megegyező tartalmú minősített adattal való visszaélés pedig bűncselekményt[42] valósít meg.

Az információgyűjtés lehetősége a magánszektor, a biztonsági szféra számára is adott, de az eszközökhöz, módszerekhez való hozzáférhetőség mértéke megkülönbözteti a nemzetbiztonsági szervek által végzett tevékenységtől. Az állami monopólium csak az adatvédelem általános szabályain túlmutató magánszférába történő beavatkozás esetén válik egyértelművé, így azokban az esetekben, amikor az információgyűjtő az Infotv. rendelkezéseit tiszteletben tartja, az érintettekről, akár tudtuk nélkül is gyűjthetőek információk. A nemzetbiztonsági szolgálatok operatív tevékenységére külső szemlélőként

---

[37] Más néven az OSINT-tevékenység (Open Source Intelligence), ami a nyílt forrásból származó információk gyűjtését, feldolgozását, értékelését, osztályozását és terjesztését jelenti. Lásd: UNICSOVICS György: *OSINT - Helye, szerepe a titkosszolgálatok világában*, Open Source Intelligence Konferencia, Nemzeti Közszolgálati Egyetem, 2013. október 3., http://mibeinfo.hu/13-konferencia-open-source-intelligence-informaciogyujtes-es-feldolgozas-nyilt-forrasokbol/ (utolsó megtekintés: 2018. 09. 23.)

[38] Az OSINT-tevékenységből származó adatok a megszerzett információknak nagyjából a 80%-át teszik ki, míg a más hírszerzési ágak tevékenységéből származó adatok együtt jelentik a fennmaradó 20%-ot. Lásd: KOBOLKA ISTVÁN: *Nemzetbiztonsági alapismeretek.* Nemzeti Közszolgálati és Tankönyv Kiadó. Budapest, 2013. 117. p.

[39] Jóhiszeműen eltekintve a jogellenes, engedély nélküli hozzáférés, feltörés lehetőségétől.

[40] Nbtv. 53–62. §.

[41] Például Big Data technológiával elemzett adatok (Big Data Analytics, BDA) esetében. Lásd: CHIANG et al.: *Special Issue: Strategic Value of Big Data and Business Analytics*, Journal of Management Information Systems, 2018/2(35). 384. p.

[42] Minősített adattal visszaélés, 2012. évi C. törvény a Büntető Törvénykönyvről (a továbbiakban Btk.). 265. §.

kevés rálátási lehetőség van, ezért a törvényi szabályozás által megfogalmazott rendelkezések jelentik az egyedüli forrást.

Abból kiindulva, hogy a vezető titkosszolgálati hatalomnak tekinthető Amerikai Egyesült Államok is egyre inkább támaszkodik a magánszektorra a hírszerzési műveletek kivitelezése során,[43] feltételezhető, hogy ha jelenleg nem is, de a jövőben Magyarországon is megjelenik az igény az ilyen típusú együttműködésre.[44] Számos olyan egyesület, vállalat létezik, amelyek fő tevékenységi körét az információkhoz való hozzáférés keresése, információbrókeri, adatbányászati és adathalász tevékenységek végzése jelenti. A szakmai hozzáértés és a releváns vállalati profil miatt, a nemzetbiztonsági szervek az ilyen tevékenységeket végző szervezeteket potenciálisan információgyűjtésre alkalmasnak minősíthetik. E mellett az Infotv. szerinti közzétételi kötelezettség alóli mentesülés is előnyös, hiszen olyan magántulajdonban lévő cégekről beszélünk, amelyeknek az állami szervekkel történő összefonódása rejtve marad, ezáltal az állampolgárok a közérdekű adatok megismeréséhez való jogukat sem tudják érvényesíteni.[45] Ha ennek a magánszféra és a személyes adatok védelméhez kapcsolódó oldalát tekintjük, a nemzetbiztonsági szervek titkos információgyűjtő tevékenységének jogkorlátozó volta csak az állami, nemzetbiztonsági érdekre és eljárásra való tekintettel felel meg a szükségességi és arányossági kitételnek. A kifejezetten törvényi engedélyen alapuló és a törvényességnek megfelelő titkos információszerzés a magánszektor részére akkor sem adott, ha ezt nemzetbiztonsági szerv kérelmére és állami érdekből történik.

A titkos információgyűjtő tevékenység kivitelezésének előfeltétele, hogy a nyílt forrásból származó információgyűjtés elégtelen, nem megfelelő mennyiségű vagy minőségű adathoz való hozzáférést mutasson.

2. Külső engedélyhez nem kötött titkos információgyűjtés

Titkos információgyűjtés alatt az a cselekmény értendő, amikor a törvény által felhatalmazott szervek[46] a nemzetbiztonsági jelleg leplezésével, az érintett tudta nélkül szereznek be információkat, személyes adatokat. Ennek körében megkülönböztetendő a külső engedélyhez kötött és a külső engedélyhez nem kötött információgyűjtés. Az Nbtv. 58. § (6) bekezdés értelmében „az engedélyező eljárásáról, illetve a titkos információgyűjtés tényéről az érintettet nem tájékoztatja.” A Társaság a Szabadságjogokért

[43] SZALAI GÁBOR: *A nemzeti hírszerzés és a magánszektor kapcsolatának alapkérdései az USA-ban.* Hadtudományi Szemle 2008/1(2). 22. p.

[44] A magán-titkosszolgálati vállalkozások, magánszemélyek általi megbízás alapján történő titkos információgyűjtő tevékenysége már hazánkban is megjelent és erősödő tendenciát mutat. LÉNÁRT FERENC: *Magán titkosszolgálatok hazai megjelenése és működése.* Hadtudomány 2008/3-4. 2. p.

[45] Amennyiben mégis nyilvános az együttműködés, közérdekű vagy közérdekből nyilvános adat nemzetbiztonsági érdekre történő hivatkozás esetén minősített adattá módosítható, így egy esetleges közérdekű adatigénylés is jogszerűen megtagadható.

[46] Titkos információgyűjtésre felhatalmazott állami szervek: Információs Hivatal, Alkotmányvédelmi Hivatal, Katonai Nemzetbiztonsági Szolgálat, Terrorelhárítási Központ, Nemzetbiztonsági Szakszolgálat, Rendőrség, Ügyészség, Nemzeti Adó- és Vámhivatal, Nemzeti Védelmi Szolgálat, http://www.nbsz.gov.hu/?mid=19, (utolsó megtekintés: 2018. 08. 11.)

(TASZ) civil jogvédő szervezet véleménye szerint[47] az önrendelkezési jogból kifolyólag a titkos információgyűjtés végeztével szükséges lenne az érintettet tájékozatni[48] a vele szemben történt információgyűjtés tényéről, legfőképp abban az esetben, ha az információgyűjtés eredménye nem kielégítő, nem összevethető a kért hírigénnyel, feltevéssel.

Az Nbtv. 54. §-ban felsorolt esetekben, a külső engedély mellőzésének lehetősége a magánszféra csekélyebb mértékű sérelmére vezethető vissza, így az engedélyezése az adott szolgálat főigazgatójának a hatáskörébe tartozik.

2. 1. Felvilágosítás kérése [Nbtv. 54. § (1) a)] és a nemzetbiztonsági jelleg leplezésével történő információgyűjtés [Nbtv. 54. § (1) b)]

A nemzetbiztonsági ellenőrzés kivitelével, amennyiben a kért információszolgáltatásnak a nemzetbiztonsági jellegű célja leplezve van, senki sem kötelezhető adatszolgáltatásra. Ha az érintett tudta nélkül, egy harmadik személytől[49] származnak a rá vonatkozó, másod- vagy akár harmadkézből származó információk, akkor sem a személyes adatok kezelésének céljáról történő előzetes tájékoztatás, sem az érintett részéről, az adatok kezeléséhez szükséges önkéntes és egyértelműen kinyilvánított beleegyezés nem történik meg. Az Nbtv. 54. § (1) a) és b) pontja szerinti felvilágosítás kérése és a nemzetbiztonsági jelleg leplezésével történő információgyűjtés, az ún. puhatolás[50] esetében, véleményem szerint, információhoz való hozzájutáshoz jogalapot az Nbtv. ezen szakasza csak az érintettől, és nem bárkitől származó adatok esetében szolgáltat, tekintve, hogy kétes adatokra alapozva, az ezek alapján indult operatív eljárások eredményének megbízhatósága is kérdéses lehet.

2. 2. Titkos kapcsolat létesítése magánszeméllyel [Nbtv. 54. § (1) c)]

A magánszeméllyel kialakított információszerző kapcsolat magában hordozza a harmadik személy haszonszerzésének lehetőségét is. Az önkéntesen együttműködő magánszemély ideológiai-elvi alapon, büntetlenségi megállapodás keretében[51] vagy akár anyagi ellenszolgáltatásért is vállalhatja az adatok szolgáltatását. Ez utóbbi, ha pozitivista szemléletből tekintjük, jogi problémát ugyan nem vet fel, hiszen egy törvényileg engedélyezett és bevett eljárás. Ezzel szemben komoly kérdésként jelentkezik a személyes adatokért cserébe történő anyagi ellenszolgáltatásnak az a vetülete, hogy ezzel a titkos információgyűjtést végző szolgálatok látszólag beárazzák a személyes adatokat. Ezt továbbgondolva, amennyiben a magánszemélyektől szerzett információért

[47] Társaság a Szabadságjogokért: Vélemény a Belügyminisztérium nemzetbiztonsági szolgálatokról szóló törvény és az információs jogi törvény módosításával kapcsolatos, BM/8652/2017. számú előterjesztéséről, https://tasz.hu/files/tasz/imce/2015/nbtv_velemeny.pdf (utolsó megtekintés: 2018. október 15.)

[48] Az állampolgárok értesítését többek között a szomszédunkban elhelyezkedő Horvát Köztársaságban is törvény írja elő, így nem egy újszerű kezdeményezésről van szó. Lásd.: BODA JÓZSEF: *„Szigorúan titkos!"?* Nemzetbiztonsági almanach. Zrínyi Kiadó. 2016. 179. p.

[49] Infotv. 3. § (22) „*harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek."*

[50] RÁCZ LAJOS: *A titkos információszerzés néhány elméleti kérdése.* Szakmai Szemle – A Katonai Biztonsági Hivatal Tudományos Tanácsának Kiadványa 2010/3. 18. p.

[51] Amennyiben az Nbtv. 55. §-ban foglalt részletszabályoknak az együttműködő személy megfelel.

nem minden egyes esetben ugyanannyi ellenszolgáltatás járna, arra lehetne gondolni, hogy nem egyforma az érintettek személyes adatainak az abszolút értéke,[52] míg a magánszféra-sérelem mértéke megegyezik. Természetesen a szolgálatok által megszerezni kívánt adatok hasznossága nem összemérhető, de az információs önrendelkezési jog általi védelem, mint az emberi méltóságból levezett és nevesített jog, nem tehet különbséget az érintettek adatainak értéke között, mindenkit egyenlő mértékben illet meg.[53]

2. 3. A nemzetbiztonsági jelleg leplezése céljából fedőokmány készítése és használata [Nbtv. 54. § (1) f)]

A külső engedélyhez nem kötött műveletek engedélyezése az adott szerv főigazgatójának a hatáskörébe tartozik, azonban az Nbtv. 54. § (2) alapján, „rendvédelmi szerv (…) fedőintézményként, okmánya fedőokmányként csak az illetékes miniszter és az érintett szervezet országos vezetőjének tájékoztatásával alkalmazható." [54] Személyes adatok beszerzése céljából készített és használt fedőokmány birtoklása esetén is figyelme kell venni a célhoz kötöttséget, illetve a cél megvalósulását vagy lehetetlenülését, aminek bekövetkezte után személyes adatok gyűjtése végett nem használható fel titkos információgyűjtés során a fedőokmány. Azonban a törvény nem részletezi a használatára adott maximális időtartamot, egyedül a belső engedélyben feltüntetett határnap jelenti a korlátozó tényezőt. Valamint, mivel belső engedélyhez kötött a használata, nem vonatkozik rá a kétszer 90 napos, külső engedélyhez kötött tevékenységekre irányadó időintervallum sem. Egy hipotetikus példán szemléltetve az engedélyezéssel kapcsolatos problémát: amennyiben a fedőokmány birtoklója a használatára bocsátott iratot, a belső engedélyben feltüntetett időponton túl is információgyűjtés céljából használná, nem valósítaná meg a Btk. 307. § alapján a jogosulatlan titkos információgyűjtés bűntettét, tekintve, hogy a büntetőtörvény csak a külső engedélyhez, azaz bíró vagy az igazságügyért felelős miniszter engedélyéhez kötött titkos információgyűjtés esetkörében nevesíti ezt a tényállást.

2. 4. Lakás, egyéb helyiség, bekerített hely, nyilvános vagy a közönség részére nyitva álló hely, illetve jármű titokban történő megfigyelése, észleltek rögzítése; [Nbtv. 54. § (1) h)] és (nyilvános vagy a közönség részére nyitva álló helyen történő) beszélgetés lehallgatása, technikai úton történő rögzítése [Nbtv. 54. § (1) i)]

Nyilvános vagy mások számára is nyitva álló helyiségben,[55] illetve eseményen történő titkos megfigyelés esetén, pont a nyilvánosság miatt, számolni kell azzal a ténnyel, hogy a megfigyelt személy nagy valószínűséggel nem egyedül tartózkodik a helyszínen,

---

[52] Természetesen a szolgálatok szemszögéből az adatok értékei nem azonosak, de arra tekintettel, hogy az önrendelkezési jog ugyanakkora sérelmet szenved egy ugyanolyan adat kiadásával, így ennek a honorálása is ugyanolyan mértékben szabályozott kellene legyen.

[53] *„Ahogy az emberek nem szabadforgalmú javak, ugyanúgy az emberek magánszférájának egyes elemei, köztük a rájuk vonatkozó személyes információk sem lehetnek azok."* SZABÓ MÁTÉ DÁNIEL: *Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival.* Információs társadalom 2005/5(2). 47. p.

[54] Nbvt. 54. § (2).

[55] *„Nyilvánosnak minősül az a helyiség vagy terület, amelyet bárki szabadon felkereshet, míg a közönség számára nyitva állónak minősül az a helyiség vagy terület, amelyet meghatározott feltételeknek eleget téve – vagy anélkül – bárki felkereshet."* Lásd: DOBÁK IMRE: *A nemzetbiztonság általános elmélete*, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet. Budapest, 2014. 226. p.

vagy vesz részt eseményen. Ebben az esetben olyan személyek adatai is a megfigyelés tárgyává válhatnak, akikkel szemben az adatgyűjtésnek nincs sem törvényes célja, sem jogalapja. A nyilvános helyiségekben történő beszélgetések nem tartoznak az Nbtv. 56. § hatálya alá, így külső engedély nélkül is lehallgathatók és rögzíthetőek. A felvázolt problémakör, miszerint nyilvános környezetben, olyan személyek is információgyűjtő tevékenység alanyává válhatnak, akik esetében erre nincs törvényes alap, a nyilvános helyen történő beszélgetések lehallgatásakor és rögzítésekor is felmerül.

3. Külső engedélyhez kötött titkos információgyűjtés

Azokat a törvény által meghatározott titkos információgyűjtő tevékenységeket, amelyek a magánszférát, személyiségi jogokat jelentősebb mértékben korlátozzák vagy sértik, csak külső engedély alapján jogszerű lefolytatni. Az adott szerv főigazgatói előterjesztése után az engedélyezési kérelmet a Nemzetbiztonsági Szakszolgálat főigazgatója nyújtja be. Az engedélyező a Fővárosi Törvényszék elnöke által e feladatra kijelölt bíró, illetve az igazságügyért felelős miniszter lehet.[56]Kivételes engedély[57] esetében a főigazgató is engedélyezheti a törvényben szabályozott feltételek[58] megléte esetén a titkos információgyűjtést, de csak korlátozott ideig,[59] és ugyanabban az ügyben csak egyetlen alkalommal. A főigazgatói előterjesztésnek tartalmazni kell az engedélyezendő információgyűjtés helyszínét, az érintett(ek) nevét, a szükségesség indokát, valamint azt az időintervallumot is, amely során előreláthatólag az információgyűjtés történni fog.

Az engedélyező bíró vagy miniszter maximálisan 90 napban szabhatja meg az információgyűjtésre rendelkezésre álló időtartamot, azonban indokolt esetben lehetőség van ezt további 90 nappal meghosszabbítani. A törvény az információgyűjtés megszűnésének az eseteit is megnevezi, mégpedig, ha az a célját elérte, ha nem várható tőle eredmény, ha hosszabbítás nélkül lejár a 90 napos időtartam, illetve, ha valamilyen oknál fogva az információk gyűjtése törvénysértő.[60] Ezzel összefüggésben szükséges megemlíteni az Alkotmánybíróság 9/2014. (III. 21.) AB határozatában közzétett állásfoglalását, amely alkotmányellenesnek nyilvánította a nemzetbiztonsági szolgálati jogviszony létrejötte utáni folyamatos nemzetbiztonsági ellenőrzést, amelynek keretében évente kétszer 30 nap időtartamig titkos információgyűjtés[61] is folytatható lett volna a szolgálat hivatásos állományú tagjával szemben.

A külső engedélyhez kötött titkos információgyűjtéshez a lakás és gépjármű átkutatása és az észleltek rögzítése, a lakásban és személygépjárműben történt események megfigyelése és rögzítése, postai küldemény felbontása, ellenőrzése és tartalmának rögzítése,

---

[56] Nbtv. 58. §.
[57] Nbtv. 59. §.
[58] Az engedélyező döntéséig, és csak abban az esetben, ha a késedelem a nemzetbiztonsági szolgálat eredményességét veszélyeztetné.
[59] Mivel az engedélyező az engedély benyújtásától számított 72 órán belül határozatot hoz, ezért kivételes engedély esetében ez egyben a maximális időtartam is, amelyet információgyűjtésre a főigazgató engedélyezhet.
[60] Nbtv. 60. § (1).
[61] 2013. évi LXXII. törvény 9. és 13. § (ebben a formában nem lépett hatályba).

elektronikus hírközlési szolgáltatás útján továbbított kommunikáció tartalmának megismerése és rögzítése, és az ehhez szükséges technikai eszköz elhelyezése tartozik.

3. 1. A lakás vagy jármű titokban történő átkutatása és az észleltek rögzítése [Nbtv. 56. § a)] és a lakásban vagy járművön történtek megfigyelése, ill. rögzítése [Nbtv. 56. § b)]

A magánlakásra vonatkozó a) pontot összevetve az Nbtv. 54. § (1) h) pontjával, amely a lakást, nyilvános vagy a közönség részére nyitva álló helyet, illetve járművet is megfigyelési területnek nyilvánítja; látható, hogy a két megjelölt törvényhely teljes lefedettséget biztosít, nincs olyan terület vagy helyiség, amelyet ne lehetne információgyűjtésre használni, akár az adott szerv főigazgatójától származó, akár külső engedély alapján. Az 1813/T/2008-4. ügyszámú, a nemzetbiztonsági szolgálatok külső engedélyhez kötött titkos információgyűjtéséről szóló adatvédelmi biztosi ajánlás alapján, az ilyen jellegű titkos információgyűjtés csak akkor nem sértené a célhoz kötöttség elvét, ha meghatározott személyazonosságú érintettekre vonatkozna az engedély, hiszen jelenleg elégséges az érintettek nevét és körét megadni. Kérdéses, hogy egy személy körébe ki tartozik pontosan. A lakásban történő események megfigyelése során, azok a beszélgetések is lehallgathatóak, amelyek nem tartoznak az Nbtv. 54. § (1) i) pontja alapján engedélyezettek közé, így akár kiskorú személyek különleges adataihoz[62] is biztosított a hozzáférés. Ebből kifolyólag az autonómiának az Alkotmánybíróság által megfogalmazott érinthetetlen lényege csupán egy absztrakt lehetőség, hiszen a valóságban ennek nincs semmilyen földrajzi, fizikai kivetülése.

3. 2. Postai küldemény felbontása, ellenőrizése és tartalmának rögzítése [Nbtv. 56. § c)]

A posta útján értelmezett csomag,[63] illetve levél,[64] és annak tartalma, mint levéltitok, az Emberi Jogok Európai Bírósága értelmezésében Az emberi jogok és alapvető szabadságok védelméről szóló egyezmény 8. cikkében lefektetett magán- és családi élet tiszteletben tartásához való joghoz tartozik. Problémásnak mutatkozik, a levél formátumban érkező, kórházi-, szűrővizsgálati eredményről szóló értesítéseket, egészségügyi adatokat tartalmazó levelekhez való korlátlan hozzáférés lehetősége, hiszen az ezekből nyert információk érintettel szembeni felhasználása arányosnak[65] aligha, és etikusnak semmiképp sem tekinthető, illetve a levél ismeretlen tartalmából kifolyólag a célhoz kötöttség is megkérdőjelezhető.

---

[62] Infotv. 3. § 3) 3. *„különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok."*

[63] 2012. évi CLIX. törvény a postai szolgáltatásokról, 2. §, 29. *„postacsomag: kereskedelmi értékekkel rendelkező vagy nem rendelkező árut, tárgyat tartalmazó könyvelt postai küldemény."*

[64] 2012. évi CLIX. törvény a postai szolgáltatásokról, 2. §, 24. *„levélküldemény: az a postai küldemény, amely írásos formában megjelenített, vagy fizikai adathordozón rögzített egyedi vagy személyes jellegű közlést, adatot vagy információt tartalmaz."*

[65] Az egészséghez való jog az élethez való jogból lett nevesítve, amely az információs önrendelkezési joggal szemben korlátozhatatlan.

3. 3. Elektronikus hírközlési szolgáltatás útján továbbított kommunikáció tartalmának megismerése és rögzítése [Nbtv. 56. § d)]

Az infokommunikációs lehetőségek folyamatos fejlődése a jogszabályi háttér megújításait is maga után vonja. Napjainkban az elektronikus kommunikáció fogalmát nem meríti ki a telefon használata, számos egyéb lehetőség is adott, amelyeket így az elektronikus hírközlési szolgáltatás útján továbbított kommunikáció kifejezés magában foglal.

2016. VII. 17-től hatályos a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről szóló 185/2016. (VII. 13.) Korm. rendelet, amelynek már az elnevezése is kissé félrevezető, tekintve, hogy csak az a digitális kommunikáció nem titkosított legalább alapvető szinten, amelyet az érintett nem szándékozik titokban[66] tartani. A kormányrendelet által az együttműködésre kötelezettek tekintetében a 2003. évi, az elektronikus hírközlésről szóló C. törvény meghatározza a titkos információgyűjtés fogalmát: „az elektronikus hírközlő hálózaton és elektronikus hírközlő eszközökkel az elektronikus hírközlési tevékenység során, illetve azzal összefüggésben keletkezett, továbbított információk, adatok kiválasztása, kicsatolása, technikai eszközzel történő rögzítése és megismerése az arra jogosult szervek által.[67]" A kormányrendelet nem csak a kifejezetten kommunikációra létrehozott felületeket, hanem az alkalmazásszolgáltatókat[68] is a titkos információgyűjtő tevékenységek céljából együttműködő szervek körében rögzíti, így a szolgáltatók a felhasználók metaadatait[69] kötelesek egy évig megőrizni és a Nemzetbiztonsági Szakszolgálat kérésére átadni. Ez alól nem jelent kivételt a szolgáltató metaadatokkal kapcsolatos ismeretének hiánya sem, ez esetben a jövőre nézve kötelesek az adatok rögzítésére.

A jogi szabályozás kiterjedtségének kezelésére és a nemzetközi lehallgatási botrányok hatására, a szolgáltatók és az érintett részére is a legbiztonságosabb titkosítási lehetőség a felhasználó eszközén történő végponti titkosítás, így hiába van az adatszolgáltató információátadásra kötelezve, ennek kivitelezése számára lehetetlen. Azonban a kormányrendelet 3. § (5) bekezdése alapján, az együttműködő „alkalmazásszolgáltató nem végezhet olyan rendszer-, illetve szolgáltatásfejlesztést, valamint nem hajthat végre olyan szervezeti átalakítást, amely a titkos információgyűjtést kizárja vagy más módon ellehetetleníti." Ezzel a szabályozással azok a szolgáltatók, akik eddig nem végponti titkosítást használtak, nem is tudnák a jövőben ilyen módon átalakítani a szolgáltatásaikat a felhasználói körből származó, erősödő érdeklődésre való tekintettel sem. Azonban a digitális adatvédelem egyre nagyobb térhódítása miatt, a tudatos felhasználók keresik azokat a

---

[66] Például közösségi oldalakon, a mindenki által látható, elérhető bejegyzések és az ezekre adott válaszok, de ezzel szemben a privát üzenetváltások már a titkosított kategóriába tartoznak.

[67] 2003. évi C. törvény az elektronikus hírközlésről 188. § 105.

[68] 185/2016. (VII. 13.) Korm. rendelet, 1. § a) *„alkalmazásszolgáltató: az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) szerinti titkosított kommunikációt biztosító alkalmazásszolgáltató."*

[69] 2001. évi CVIII. törvény, 13/B. § (2) *„A külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén a titkosított kommunikációt biztosító szolgáltatást nyújtó alkalmazásszolgáltató a) a szolgáltatás típusát; b) a szolgáltatás előfizetőjének vagy felhasználójának ba) a szolgáltatás igénybevételéhez szükséges azonosító adatait, a szolgáltatás igénybevételének dátumát, kezdő és záró időpontját; bb) a regisztrációhoz használt IP-címét és portszámát; bc) az igénybevételnél használt IP-címét és portszámát; c) a felhasználói azonosítót köteles átadni."*

lehetőségeket, amelyek biztosítják számukra a megfelelően védett környezetet, így valószínűsíthető a végponti titkosítást nyújtó szolgáltatások használatának a fellendülése.

Külön kérdésként jelentkezik az elektronikus hírközlési szolgáltatás útján továbbított kommunikáció megismerése és rögzítése kapcsán az úgynevezett követő lehallgatás[70] esetköre. Ennek során a lehallgatott személynek előzetes gyanúja van az őt ért megfigyelésről, ami miatt a kommunikációja biztosítása érdekében az általa használt elektronikus eszközöket folyamatosan cseréli. Mivel a szolgálatokat nem egy adott telefonon történt kommunikáció érdekli, hanem kifejezetten a célszemélyt érintő körülmények és beszélgetések miatt tartják megfigyelés alatt, így az új kommunikációs eszköz is lehallgatásra kerül. Ezzel kapcsolatosan az engedély tartalma okozhat gondot, hiszen ha egyedileg azonosítható eszközre[71] adják, a készülék időközben más állampolgárhoz kerülhet, akire nézve már nincs engedélyezve a lehallgatás, ha pedig lehallgatható személy alapján történik az engedélyezés, akkor az a kérdés, hogy csak az engedélyezési időkeret szab határt vagy a lehallgatott csereeszközök száma is korlátozva[72] van.

3. 4. Információs rendszerben kezelt adatokat megismerése és tartalmának rögzítése, valamint az ehhez szükséges technikai eszköz elhelyezése, illetve elektronikus adat az információs rendszerben történő elhelyezése [Nbtv. 56. § e)]

Az Nbtv. 56. § e) pontja a teljes hálózati forgalomhoz való hozzáférést biztosítja, amelyet az online házkutatás[73] fogalmával azonosíthatunk. Az online házkutatás alatt értendő a személy minden olyan elektronikus eszközén tárolt adatának a megismerése, rögzítése és felhasználása, amelyek tulajdonképpen a kémprogramok telepítése által elérhetőek. Az adattárolás alatt nem csak a fizikai adattárolók értendők, hanem a felhő alapú tárhely szolgáltatások[74] használata is, amelyek esetében még az általános adatvédelmi szabályok is változóban vannak, kiforratlanok. Könnyen belátható, hogy az adatokhoz való hozzáférés mértéke nem arányos a magánszférát ért sérelemmel, mivel a napjainkban szinte nincs olyan személyes adatunk, ideértve a különleges adatokat is, amelyeket akár számítógépeken, akár valamilyen adattároló eszközön, felhőben ne tárolnánk saját használatra. Állampolgári bejelentés kivizsgálása miatt, a Nemzeti Adatvédelmi és Információszabadság Hatóság a nemzetbiztonsági célból használt kémprogramokkal kapcsolatban, 2014-ben adott ki egy Jelentést,[75] amelyben a kémprogramok alkalmazásának jogi hátterét és adatvédelemi kérdéseit részletezi. Habár a Jelentésben

[70] TAKÁCS GERGELY: *Big data (adatvezérelt) elemzési módszerek alkalmazása a nemzetbiztonsági szférában.* Terror & Elhárítás 2018/1. 25. p.

[71] A telefonok esetében a SIM kártya azonosítása csak az egyik lehetőség, hiszen maga a készülék is rendelkezik egy egyedi számsorral, amellyel egyértelműen beazonosíthatóak, ezt IMEI (International Mobile Station Equipment Identity) számnak nevezzük.

[72] Erre nézve nincsenek nyilvánosan elérhető információk, de a költséghatékonyság biztosítása érdekében, elképzelhetőnek tartom a csereszközök számának engedélybeli maximalizálást is.

[73] DOBÁK IMRE: *Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében.* Hadmérnök 2017/2(12). 239. p.

[74] „*Az informatikai ipar felhő technológiának nevezi azokat a megoldásokat, amelyek lehívásos hálózati hozzáférést tesznek lehetővé távolban lévő, konfigurált számítógépes források (hálózatok, szerverek, alkalmazások, szolgáltatások, tartalmak) gyűjteményéhez*." FALUDI GÁBOR–GRAD-GYENGE ANIKÓ: *A cloud computing-alapú szolgáltatások szerzői jogi megítéléséről,* Infokommunikációs és Jog, 2012/3(50), 105. p.

[75] NAIH-1904-6/2014/T ügyszámú jelentés, a kémprogramok magyar nemzetbiztonsági célú alkalmazásáról

az előadó megállapította, hogy a nemzetbiztonsági szervek a titkos információgyűjtésre használt „kémprogram alkalmazásával kapcsolatban a törvényi előírásokat maradéktalanul betartva hajtja végre", elgondolkodtató az az általános bizalmatlanságot kifejező körülmény, miszerint a laptopokon található, gyárilag beépített webkamerát a felhasználók többsége használaton kívül eltakarja.[76]

Az online házkutatásokon felül, a nemzetbiztonsági szolgálatoknak a biometrikus adatokhoz való hozzáférése is aktuális kérdés, amelynek előzményeként tekinthető, hogy 2015. XI. 27-én hatályba lépett a 2015. évi, az arcképelemzési nyilvántartásról és az arcképelemző rendszerről szóló CLXXXVIII. törvény. Ebben részletes van szabályozva, hogy a nemzetbiztonsági szervek közül, melyik szerv, milyen célból férhet hozzá a nyilvántartott adatokhoz és elemező rendszerhez, azonban a jelenlegi megfogalmazás az általános, és nem az egyedileg megadott jogosultságot feltételezi. Véleményem szerint legalább belső, főigazgatói engedélyhez kell kötni egy olyan adatbázisnak a titkos információgyűjtés céljából való hozzáférési lehetőségét, amely a jövőben csaknem minden magyar állampolgár arcképmását[77] és arckép profilját[78] tartalmazni fogja.

4. Engedélyezési lehetőségek

4. 1. Bírói engedély alapján

A bírói engedély alapján történő titkos információgyűjtés esetei – amelyek a végrehajtó hatalmi ág engedélyezésének a területén kívül helyezkedik el, – az Nbtv. 58. § alapján az Alkotmányvédelmi Hivatal és a Katonai Nemzetbiztonsági Szolgálat tevékenységeinek egy része. Érdekes kérdést vetne fel az engedélyek kiadásról vagy megtagadásáról szóló statisztikai kimutatás nyilvánosságra hozatala, mert a végrehajtó hatalmon kívüli törvényességi kontrollt egyedül a kijelölt bíró általi engedélyezések jelentik. Ezzel demonstrálni lehetne, hogy tényleges garanciát jelent a bírói engedélyezés és nem csak egy bürokratikus, a kivitelezéshez előírt eljárási[79] elemet.

4. 2. Miniszteri engedély alapján

A miniszteri engedély alapján végzett titkos információgyűjtő tevékenységet számos kritika érte, mindez arra vezethető vissza, hogy a mindenkori igazságügyért felelős miniszter és a nemzetbiztonsági szerveket irányító miniszter ugyanannak a kormánynak

---

[76] A webkamerák eltakarásának fontosságát James Comey FBI igazgató (2013. szeptember 4-től 2017. május 9-ig) is kiemeli, mint az egyesült államokbeli kormányzati szervek által is követett gyakorlatot. l. HATTEM, JULIAN: *FBI director: Cover up your webcam.* https://thehill.com/policy/national-security/295933-fbi-director-cover-up-your-webcam (utolsó megtekintés: 2018. október 31.)

[77] 2015. évi CLXXXVIII. törvény, 1. §, b) *„arcképmás: olyan, a polgár arcképéről informatikai eszköz igénybevételével készített vagy informatikai eszköz igénybevételével feldolgozható felvétel, mely alkalmas arckép profil képzésére."*

[78] 2015. évi CLXXXVIII. törvény, 1. §, c) *„arckép profil: az arcképmásból képzett alfanumerikus adatsor, mely az annak alapjául szolgáló arcképmás rekonstruálására nem alkalmas."*

[79] Az amerikai Külföldi Hírszerzési célú Lehallgatást Engedélyező Bíróság az 1979-es megalakítása óta, a több mint 34 ezer benyújtott kérvényből 2017 végéig összesen 11 darab kérvényt utasított el, amelyből egyetlen egy volt olyan, amelyet a 2001. szeptember 11-ei terrortámadást megelőzően nyújtottak be és elutasításra került. Lásd: TAKÁCS 25.

a tagjai, így az egymás irányában történő, informális jellegű hatások nehezebben védhetőek ki, illetve ennek ellenőrizése is kétséges. Az igazságügyért felelős miniszter hatáskörébe nem csak a nemzetbiztonsági célú, hanem a terrorizmust elhárító szerv[80] bűnüldözési célú, az Nbtv. rendelkezései által szabályozott titkos információgyűjtő tevékenységének engedélyezése is beletartozik, az 1994. évi XXXIV. törvény 63. § (7) pontja alapján.

A 295/2010. (XII. 22.) Korm. rendelettel létrehozott Terrorelhárítási Központ a rendészetért felelős miniszter irányítása alá tartozik. A 1994. évi XXXIV. törvény 7/E. § (2) bekezdése értelmében a terrorizmust elhárító szerv nem gyakorol nyomozóhatósági jogkört, ellenben a 63. § (7) bekezdése feljogosítja az Nbtv. 53-60. §-ában rögzített titkos információgyűjtési tevékenységre, amelybe beleértendő, mind a külső engedélyhez nem kötött, mind a külső engedélyen alapuló információgyűjtés. Így egy olyan szerv rendőrséghez való besorolása, amely a rendőrségi nyomozóhatósági tevékenységeket nem, ellenben a nemzetbiztonsági szervek titkos információgyűjtési tevékenységét folytathatja, felveti azt kérdést, hogy egy rendőrségi szervről beszélünk vagy valójában egy olyan látens titkosszolgálati szervről, amelyet azonban az Nbtv. nem rögzít Magyarország nemzetbiztonsági szolgálatainak a körében.

5. A Szabó és Vissy kontra Magyarország ügy[81] *és hatása*

Két magyar állampolgár alkotmányjogi panasszal, az Alkotmánybírósághoz fordult a Rendőrségről szóló 1994. évi XXXIV. törvénynek a Terrorelhárítási Központra vonatkozó bizonyos szövegrészei alaptörvény-ellenességének megállapításának és megsemmisítésének ügyében. A kifogásolt szövegrészek a TEK általi titkos információgyűjtés Nbtv. alapján történő kivitelezését, azaz az igazságügyért felelős miniszter általi engedélyezését érintik, valamint ezzel párhuzamosan kifogásolták a bírói engedély mellőzésének lehetőségét is. Az Alkotmánybíróság a 32/2013. (XI. 22.) AB határozatban a kifogásolt törvényi rendelkezelések alaptörvény-ellenességének megállapítására és megsemmisítésre irányuló indítványt, a miniszteri indoklás szükségességének kivételével elutasította.

A kérelmezők az Alkotmánybíróság elutasító határozata után az Emberi Jogok Európai Bíróságához fordultak kérelmükkel, amelyben az Egyezmény 6., 8. és 13. cikkei[82] szerinti jogaik megsértését kifogásolták. A 2016. január 12-én született ítélet szerint, azzal, hogy az Alkotmánybíróság korábban érdemben vizsgálta a panaszukat, elismerte a kérelmezők lehetséges áldozati státuszát annak ellenére, hogy a titkos információgyűjtés ténye nem nyert bizonyosságot. A Bíróság egyhangúan megállapította, hogy a kérelmezőknek az Egyezmény 8. cikkén, valamint a 8. cikkével együtt olvasott 13. cikkén alapuló joga sérelmet szenvedett. Az ügy kimenetele, habár első sorban egy rendvédelmi szervre vonatkozik, a magyar nemzetbiztonsági szolgálatok szempontjából két fő jelentőséggel is bír álláspontom szerint:

[80] Azaz a Terrorelhárítási Központ titkos információgyűjtő tevékenysége.

[81] 37138/14. sz. kérelem, Emberi Jogok Európai Bírósága, Strasbourg, 2016. január 12.

[82] Emberi Jogok Európai Egyezménye (Magyarországon kihirdetve: 1993. évi XXXI. törvény az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről), 6. cikk: tisztességes tárgyaláshoz való jog, 8. cikk: magán- és családi élet tiszteletben tartásához való jog, 13. cikk: hatékony jogorvoslathoz való jog.

1. Az áldozati státusz Alkotmánybíróság általi elismerése, valamint az Emberi jogok Európai Bíróságának azon értékelése, miszerint „érintett vagy érintettek (…) köre fogalmába valóban bárki beletartozhat, így az állampolgárok tömeges és korlátlan megfigyeléséhez vezető út kikövezéseként is értelmezhető."[83] Ebből kiindulva, előrevetíthetőek a további, hasonló tartalmú állampolgári kérelmek is, amelyeket a Bíróság által megítélt 4000 eurós kártérítés is ösztönöz.

2. A Bíróság kifogásolta a miniszteri engedélyen alapuló titkos információgyűjtési lehetőséget a TEK esetében, de ez erre vonatkozó jogszabályt nem az Rtv., hanem az Nbtv. jelenti, amely főszabály szerint a nemzetbiztonsági szervekre vonatkozik. Ebből következik, hogy megfontolandó a miniszteri engedélyezés lehetőségének korlátozása a nemzetbiztonsági célú titkos információgyűjtő tevékenységek esetében is az argumentum a minori ad maius érvelés alapján. A miniszteri engedélyezés mellőzésére léteznek külföldi[84] példák, így az igazságügyi miniszter, – mint külső engedélyező – személye a folyamatból akár elhagyható is lehetne.

IV. Az információszabadság elméleti háttere

Az információs szabadságjogok másik fő részterülete az információszabadság, amely elválaszthatatlan az adatvédelemtől. Az összefüggés oka az, hogy bár az adatvédelem és információszabadság látszólag kevés közös jellemzővel rendelkezik, a céljaik egymás kiegészítését szolgálják: az információszabadság által a közhatalmi szféra átláthatóságának elérése a cél, míg az adatvédelem ezzel szemben a személyek adatainak a védelmén keresztül az állampolgárok átláthatatlanságot szolgálja.[85]

Az európai országok történelme erősen befolyásolja az adott állam információszabadsági fejlettségi szintjét, hiszen Észak- a kontinentális Nyugat-Európát[86] vizsgálva látható, hogy az első közadatokhoz való hozzáférésre vonatkozó szabályozások már korán megjelentek. Példaként említve Franciaországot, ahol az 1789-es Emberi és Politikai Jogok Nyilatkozata leszögezi, hogy „[a] polgároknak saját személyükben vagy képviselők útján joguk van e közös hozzájárulás szükségszerűségét megállapítani s azt szabadon megszavazni, valamint felhasználását nyomon követni."[87] Ennél is korábbra tehető az 1766-os svéd sajtószabadsági törvény elfogadása, amelynek következtében Svédországban az évszázadok alatt az információszabadság mélyen beágyazódott a

[83] Szabó és Vissy kontra Magyarország ügy, Emberi Jogok Európai Bírósága, 37138/14. sz. kérelem, 67. pont.

[84] Például Kanadában mindig, az USA-ban abban az esetben, ha amerikai állampolgárt érint, csak bíró engedélyezheti a titkos információgyűjtést. Lásd: DOBÁK, 61. p.

[85] PÉTERFALVI ATTILA: *Átláthatóság a védelmi igazgatásban*. Doktori értekezés, NKE. Budapest, 2014.

[86] Nagy-Britannia kivételt jelent, hiszen az első törvényük, amely erre a kérdéskörre vonatkozik csak 2000-ben lett elfogadva és 2004-ben lépett hatályba. Lásd: SZABÓ MÁTÉ DÁNIEL: *Elektronikus információszabadság külföldön*. Fundamentum. 2004/4. 123. p.

[87] Az Emberi és Polgári Jogok Nyilatkozata, 1789., http://mek.oszk.hu/00000/00056/html/228.htm (utolsó megtekintés: 2018. október 26.)

politikai kultúrába.[88] A modern kori történelem során elsőként az Amerikai Egyesült Államok fogadott el törvényt,[89] 1966-ban, kifejezetten az információszabadság szabályozása céljából. Ezen példákkal ellentétben, a posztszovjet országok esetében az állami berendezkedés nem csak a törvényi szabályozás létrejöttét, hanem az elv, és egyben a társadalmi igény kialakulását is akadályozta. Az információszabadság elvének hazai megjelenése sokáig váratott magára, hiszen a rendszerváltozást megelőző korszakban a közadatokhoz való hozzáférés lehetősége nem érvényesült, hanem épp ellenkezőleg, a közhatalom az átláthatatlan állam, átlátható polgár elvét részesítette előnyben. Az 1989-es eseményeket követően újonnan kialakult demokrácia már megfelelő alapot jelentett az információszabadság létrejöttének. Az 1989. október 23-án kikiáltott köztársaság Alkotmánya volt hazánkban az első, jogi kötőerővel rendelkező dokumentum, amely megfogalmazta a közérdekű adatokhoz való hozzáférés lehetőségét, valamint azt is, hogy a szabályozás részleteiről külön törvényt kell alkotni. Ennek elfogadása csak évekkel később történt meg, mégpedig a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény formájában, amely aztán több módosításon átesve, egészen 2011-ig hatályban maradt. E törvény érdeme az volt, hogy az adatvédelem és az információszabadság együtt kezelésének rendhagyó koncepciója mintaként szolgálhatott a kelet-közép-európai régióban később kialakuló szabályozásoknak, a hátránya viszont az, hogy megalapozta a két információs jog érvényesülésének és ismertségének eltolódását az adatvédelem irányába.[90] Ezt követően, a jelenleg is hatályban lévő, az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény részletezi a kérdéskört, valamint gyakorlásának módját az Alaptörvény VI. cikke is megfogalmazza, miszerint mindenkit megillet a közérdekű és közérdekből nyilvános adatok megismerése és terjesztése.

Az információszabadság a harmadik generációs politikai szabadságjogok közé tartozik, a sajtó- és véleményszabadságból származik, célja a közszféra transzparenciája.[91] Három fő elméleti összetevőből épül fel, amelyek maga az alapelv, a törvényi úton, pontosan szabályozott kivételek, valamint egy független ellenőrző fórum megléte.[92] A tárgya a közérdekű adat, amelynek az olyan állami, helyi önkormányzati vagy egyéb közfeladatot ellátó szerv, személy, szervezet tevékenysége során keletkezett és kezelésében lévő adatok minősülnek, amelyek nem tartoznak a személyes adatok fogalmi körébe.[93] A közérdekből nyilvános adatok azok, amelyek nem sorolhatóak a közérdekű adatok közé, de a közérdekűségükre tekintettel nyilvánosságra hozandóak, ilyenek lehetnek például a közfeladatot ellátó személyek meghatározott személyes adatai. A közadatok megismerésének vannak korlátai, az Infotv. alapján „[a] közérdekű és közérdekből nyilvános adatok megismeréséhez való jogot (…) törvény honvédelmi érdekből;

[88] BANISAR, DAVID: *Freedom of information around the world 2006.* http://www.freedominfo.org/documents/global_survey2006.pdf, (utolsó megtekintés: 2018. október 3.)
[89] Freedom of Information Act (FOIA), 1966. július 4. USA.
[90] SZÉKELY IVÁN: *Fórum*, Fundamentum 2004/4. 53. p.
[91]: *„az információszabadság alapjogának abban az összefüggésében kell vizsgálni, hogy a jogállamban az állam működésének a polgárok számára átláthatónak, "áttetszőnek" kell lennie”*. 60/1994. (XII. 24.) AB határozat, ABH 1994. 342., 351.
[92] SÓLYOM LÁSZLÓ: *Egy új szabadságjog: az információszabadság*, Valóság, 1988/9. 1. p.
[93] *„Az információ csak akkor nem tekinthető közérdekűnek, ha az személyes adat.”* 32/1992. (V. 29.) AB határozat. ABH 1992. 182., 185.

nemzetbiztonsági érdekből; bűncselekmények üldözése vagy megelőzése érdekében; környezet- vagy természetvédelmi érdekből; központi pénzügyi vagy devizapolitikai érdekből; külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra tekintettel; bírósági vagy közigazgatási hatósági eljárásra tekintettel; a szellemi tulajdonhoz fűződő jogra tekintettel korlátozhatja."[94]

A közadatokhoz való hozzáférésnek két eltérő módja van, mégpedig a közérdekű adatot kezelő szerv közzétételi kötelezettsége, valamint az állampolgárok által benyújtható közérdekű adatigénylések lehetősége. Az állami szervek a közzétételt a közzétételi listán, „internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, kinyomtatható és részleteiben is adatvesztés és - torzulás nélkül kimásolható módon, a betekintés, a letöltés, a nyomtatás, a kimásolás és a hálózati adatátvitel szempontjából is díjmentesen"[95] kell közzétegyék. Megkülönböztetünk általános, különös és egyedi közzétételi listát, amelyek a tartalmuk alapján különíthetőek el. Az általános közzétételi listán szereplő adatok körét az Infotv. 1. melléklete szabályozza. Ezen kell feltüntetni a közfeladatot ellátó szerv elérhetőségét, postai és elektronikus levelezési címét, valamint a közérdekű adatigénylések adott szervnél szokásos eljárási rendjét, illetve az információs jogokkal foglalkozó munkatárs nevét és elérhetőségét is. Az Infotv. közérdekű adatok megismeréséről szóló III. fejezete részletezi azokat a jogszabályi előírásokat, amely által bárki, a jogi érdeke igazolása nélkül állami szervtől közadatokat igényelhet.

Annak meghatározására, hogy mekkora az igénylések gyakorisága a dolgozatban tárgyalt rendvédelmi szervek tekintetében, én is a közérdekű adatigénylés eszközével (I. melléklet) kellett éljek, az adatok (II. melléklet) ugyanis sehol nincsenek hozzáférhetővé téve.

V. Az információszabadsági gyakorlat a rendvédelemben

1. Hipotézis

Az előző fejezetben bemutatottak alapján, magyar információszabadsági gyakorlatnak ezidáig szűk harminc év állt összesen rendelkezésére a fejlődéséhez. Véleményem szerint a gyakorlati szakemberek és az állampolgárok figyelmét számos, fontosabbnak gondolt alapjog foglalkoztatta ez idő alatt, mint az élethez és méltósághoz való jog a terhesség-megszakítás és az eutanázia kérdéskörei kapcsán, vagy akár a tulajdonhoz való jog szabályozása, amely a korábbi államosítás, majd később a privatizációs folyamatok során is nagy figyelmet kaptak.

A dolgozatom második fő része a magyar információszabadsági gyakorlat vizsgálata a nemzetbiztonsági szervek és a Magyar Rendőrség esetében. A közérdekű adatigényléseim válaszait formai és tartalmi szempontból fogom górcső alá venni, amely során a formai szempontot a jogszabályi előírásoknak való megfelelés, határidő betartása, válaszadási készség megléte, míg a tartalmit a feltett kérdéseimre adott érdemi válaszok,

[94] Infotv. 27. §, (2).
[95] Infotv. 33. § (1).

számadatok jelentik. Formai szempontból a részletes törvényi szabályozásból kifolyólag az adatigénylések teljes körű megválaszolására számítok, a válaszok tartalma kapcsán az az előfeltevésem, hogy a magyar lakosság adatkikérési tudatossága csekély, ritkán élnek az állampolgárok az információszabadság adta lehetőségekkel, így nem lesz jellemző a nagyobb mértékű közadatigénylés. A Rendőrség esetében a nagyobb szervezeti apparátus és a megyei tagozódás okozhat több igénylésszámot, míg a nemzetbiztonsági szervek jellemzően titkos működésének hasonló hatása lehet az adatigénylésekre.

2. Empirikus megfigyelések, tapasztalatok

2. 1. Magyar Rendőrség

Az adatigénylések gyakoriságának megállapításához első körben a Magyar Rendőrség meghatározott szerveihez nyújtottam be adatigénylést, mégpedig a 19 db megyei rendőr-főkapitánysághoz, a Budapesti Rendőr-főkapitánysághoz, az Országos Rendőr-főkapitánysághoz, a Terrorelhárítási Központhoz, valamint a Repülőtéri Rendőr Igazgatósághoz. Azért a rendőrség, és nem egy nemzetbiztonsági szolgálat részletesebb vizsgálatára esett a választásom, mert jóval nyitottabb a szervezete, rendelkezik elérhető megyei kirendeltségekkel, (feltehetően) nagyobb a hivatali apparátusa és a tevékenységi köre is közelebb áll az állampolgárok mindennapjaihoz. Mind a 23 megkeresésben ugyanazzal a kérdésekkel fordultam az illetékes szervekhez, amelyek a következők:

„1. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény „A közérdekű adatok megismeréséről szóló III. FEJEZET" hatálybalépésétől, azaz 2012. január 1. kezdő dátumtól 2017. december 31-ig bezárólag, éves bontásban, hány esetben lett közérdekű adatigénylés benyújtva (nem megkülönböztetve a természetes és jogi személyiségű kérelmezőket) a <szervezet neve> 67/2007. (XII. 28.) IRM rendelet 1. melléklete szerinti illetékességi területén.

2. Az Infotv. 30. § (3) bekezdés alapján a fent nevezett adatigénylések teljesítésének megtagadásáról az adatkezelő köteles éves bontásban nyilvántartást vezetni, így kérném számomra megküldeni, hogy 2012. január 1. és 2017. december 31. közötti időtartamban benyújtott közérdekű vagy közérdekből nyilvános adatok megismerése céljából a <szervezet neve>-nek címzett közérdekű adatigénylések közül a fent nevezett időintervallumban, évente hány alkalommal történt az adatigénylés teljesítésének megtagadása."

Az igénylés időtartama úgy lett kialakítva, hogy egész évre vonatkozzon, ezzel segítve az adatok könnyebb kezelhetőségét. A kezdő dátum az Infotv. hatálybalépésének 2012-es időpontja, a záró dátum pedig azért 2017, mert az adatigénylések benyújtása 2018. első negyedévére esett, így az utolsó teljes naptári év 2017 volt. Az igénylés az így kialakított időkeretben összesen 12 darab számadatra vonatkozott.

Már a címzettek megtalálásánál is nehézségbe ütközhetünk, ugyanis nem minden megyei rendőr-főkapitányság közérdekű adatokat tartalmazó közzétételi listája található meg a police.hu központi oldalon. Azonban a lista megtalálása sem jelent azonnali sikert, mert több esetben, a kifejezetten közérdekű adatigénylések számára fenntartott email cím hibásan van feltüntetve. Ebből kifolyólag az üzenetek kézbesítése sem lehet sikeres, csupán a megyei központi email cím elérhető e főkapitányságok esetében. Ér-

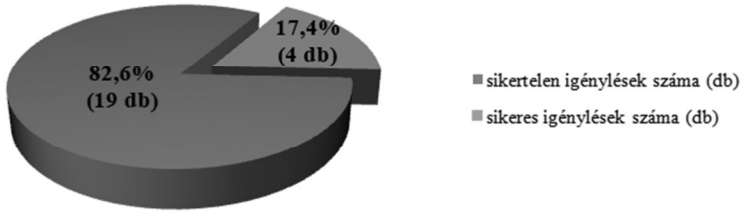
dekes módon a közérdekű adatigénylésre nem válaszoló és a hibás közzétételi listával rendelkező főkapitányságok nem estek egybe.

A 23 darab megkeresésre határidőn belül 19 válasz érkezett, 4 címzett semmilyen módon nem reagált. Az ő esetükben megnyílik a lehetőség az adatok átadásának bírósági úton történő kikényszerítésére.

Az 1. ábrán jól látható, hogy a sikeres adatigénylés mértéke 82,6 %, amelyek esetében a siker alatt a bárminemű választ értem.

1. sz. ábra

Az adatigénylés sikeressége



Forrás: saját szerkesztés.

A 23 db adatigénylés közül összesen egy címzett élt a válaszadásra előírt 15 napos határidő további 15 nappal történő meghosszabbításával, a BRFK. Az Infotv. 29. § bekezdése alapján az adatkezelőnek akkor áll módjában a határidő egyoldalú meghosszabbítása, ha „adatigénylés jelentős terjedelmű, illetve nagyszámú adatra vonatkozik, vagy az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár". Az igényelt 12 számadat nem nevezhető sem jelentős terjedelemnek, sem nagyszámú adatnak, így felvetődik az automatikus hosszabbítás gyakorlatának lehetősége, amely a válaszadásra rendelkezésre álló határidőt a kétszeresére növeli, így csökkentve a határidő túllépése miatt indult közérdekű adatigénylések megtagadása miatt indult perek számát. A válaszadás megtagadására a kézbesítéstől számított 8 napos határidő áll rendelkezésre, de ezzel a lehetőséggel nem élt egyik megkeresett sem.

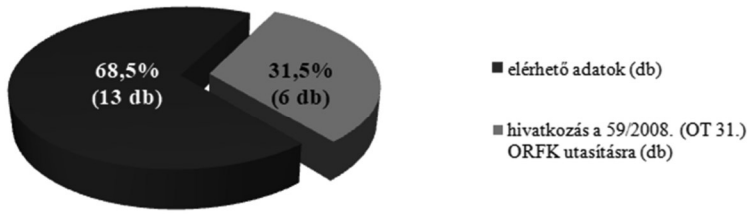
Az igénylésre érkezett 19 válaszüzenet közül 6 esetben nem sikerült az összes kért adathoz való hozzáférés. Ennek oka, hogy e szervek hivatkoztak a 2012. január 1. - 2017. december 31. közötti időszakban hatályos Rendőrség Iratkezelési Szabályzatáról szóló 59/2008. (OT 31.) ORFK utasítás 1. függelék 2013. december 31-ig hatályos 42/f., 2014. április 15-ig hatályos 42/e., valamint 2017. december 31-ig hatályos 42/d. alpontjára, miszerint a közérdekű adatok kérésével és továbbítására kapcsolatos iratok megőrzési ideje a rendőri szerveknek 1 év. Azonban azon rendőrkapitányságok gyakorlatában is ellentmondás található, akik erre az utasításra hivatkoztak, hiszen voltak, akik a 2016-os adatokat ennek ellenére csatolni tudták, és voltak olyanok is, aki csak a 2017-es adatigénylések számát közölték. Az Infotv. 30. § (3) alapján az adatigénylések meg-

tagadásáról kötelesek a szervek nyilvántartást vezetni és ezt a NAIH részére elküldeni, így az elutasított igénylések számáról egész biztosan rendelkeznek kész statisztikával, azonban a sok tekintetben eltérő mintát követő ORFK még ez esetben is hivatkozott az egy éves megőrzési időre és nem küldte el az adatokat.

Az ORFK utasításra a sikeres adatigénylések 31,5 %-a hivatkozott, tehát 6 címzett esetében (2. ábra) valóban alkalmazásra is került egy olyan belső rendőrségi utasítás, amely alapján a közérdekű adatigénylések nem teljesíthetőek és a részbeli teljesítést tartalmazó válasz üzenetben nem is térnek ki rá, hogy amennyiben nem a rendőrség, akkor ki az az adatkezelő, akitől a kért adatok beszerezhetőek.

2. sz. ábra

A sikeres adatigénylések megoszlása elérhetőség szerint



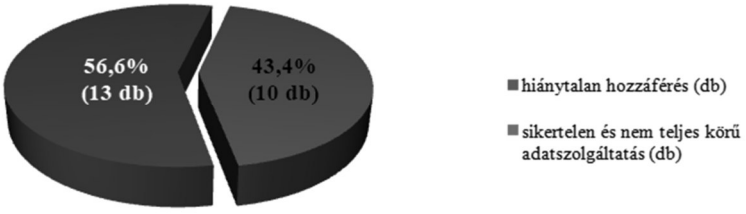
Forrás: saját szerkesztés.

Egy esetben lett kifogásolva a megyei rendőr-főkapitányság illetékessége, miszerint a területén lévő összes rendőrkapitányságtól külön-külön kellene közérdekű adatigénylést benyújtva az adatokat igényelni, ennek ellenére a kért információt mégis elküldték. Szintén egy esetben az Ügyfélkapu szolgáltatáson keresztüli beadás lehetőségét szorgalmazták, annak ellenére, hogy adatigénylés írásban vagy elektronikus úton, de akár szóban is előterjeszthető.

A fentiek alapján a 23 db közérdekű adatigénylés közül csupán 13 db, azaz 56,6% volt olyan, amely teljes körűen tartalmazta kért adatokat, míg a fennmaradó 43,4 % vagy nem válaszolt határidőn belül, illetve határidőn túl sem vagy az ORFK utasítás alapján kibújt a teljes körű válaszadás alól (3. ábra). Tehát az adatigénylés abszolút sikeressége csak 58,3%.

3. sz. ábra

A kért adatokhoz történő teljeskörű hozzáférés mértéke

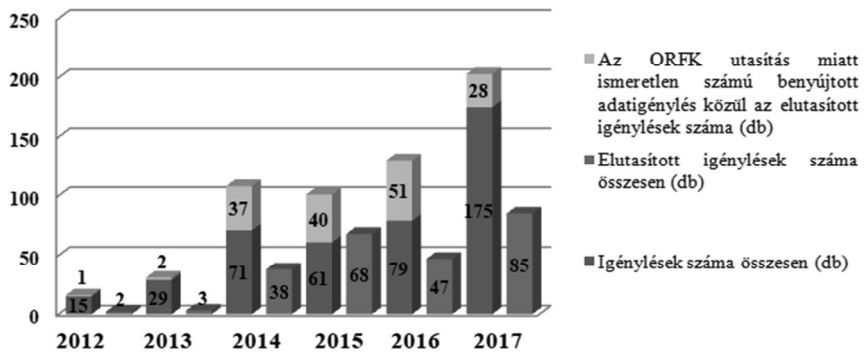


Forrás: saját szerkesztés.

Sajnálatos módon éppen az ORFK hivatkozott a legtöbb adat esetében az 1 éves megőrzési időre, pedig az előzetes várakozással megegyezően, a 2017-es év adataiból is látszódik, hogy itt a legjelentősebb az igénylések és az elutasítások száma, amelyeknek aránya 2017-ben 81,8%-os volt. Megyei szervezetekhez kevés adatigényléssel fordulnak és ezek teljesítésének megtagadása is ritkább. Bizonyos években vannak kiemelkedő igénylésszámok, de ennek hátterében valószínűsíthetően nem az információszabadság eszméjének népszerűvé és ismertté válása, hanem valamilyen helyi ügy nagyobb érdeklődést kiváltó sajtóvisszhangja áll. Olyan szervezet is van, amelyhez 5 évente egy adatigénylést nyújtanak csak be, ilyen például a Repülőtéri Rendőr Igazgatóság, amely szervezetileg ugyan az ORFK-hoz tartozik, de speciális illetékességi területe miatt külön kezelendő. Mivel az ORFK kiemelkedően sokszor hivatkozott az 1 éves megőrzési időre, így nem lehet tudni az adatigénylések pontos számát, de az elutasított igénylések számával növelve[96] az összesített számadatokat, látható, hogy a rendőrségi szervekhez benyújtott adatigénylések száma évről – évre emelkedik (4. ábra), de még így is rendkívül alacsony.

4. sz. ábra

A Magyar Rendőrség szerveihez benyújtott adatigénylések összesített száma, éves bontásban



Forrás: saját szerkesztés.

2. 2. Nemzetbiztonsági szolgálatok

A teljes lefedettség érdekében mind az öt hazai nemzetbiztonsági szervhez nyújtottam be adatigénylést, amelyek a következők: az Információs Hivatal, az Alkotmányvédelmi Hivatal, a Katonai Nemzetbiztonsági Szolgálat, a Nemzetbiztonsági Szakszolgálat, valamint a Terrorelhárítási Információs és Bűnügyi Elemző Központ. Közülük négy szerv már az Infotv. hatálybalépése előtt is létezett, a Terrorelhárítási Információs és

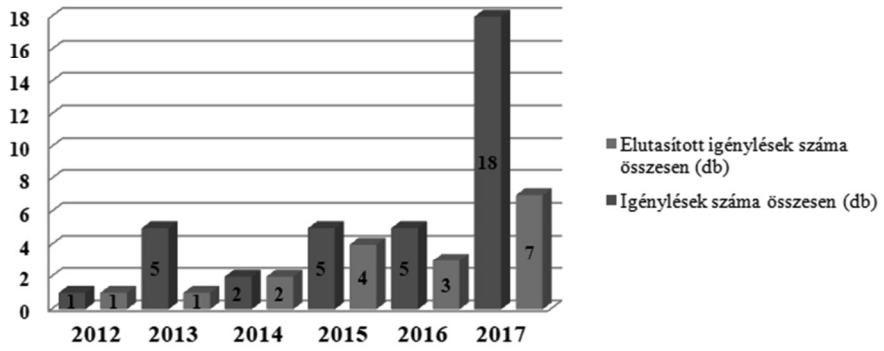
[96] Abból kiindulva, hogy amit elutasítanak, azt előzetesen be is kellett egy állampolgár nyújtsa.

Bűnügyi Elemző Központ jogelőd nélkül, 2016. július 16-án kezdte meg működését. Az adatigénylések kérdései egész évre irányultak, de ebben az esetben az alapítás évének csonkasága nem befolyásolja a statisztikát, hiszen az általam küldött igénylés volt az első, amit a TIBEK-hez benyújtottak.

Mind az öt szerv határidőn belül és teljes körűen válaszolt (5. ábra), valamint csak az Alkotmányvédelmi Hivatal kért határidő-hosszabbítást. Habár a nagyobb hatékonyság reményében az igénylésem nem tartalmazott kérdést az elutasítások indokára vonatkozóan, a szolgálatok többsége azt is megküldte. Érdekességképp jegyzem meg, hogy a Katonai Nemzetbiztonsági Szolgálat egyetlen esetben történt igénylés-elutasításának okaként az Infotv. 29. § (1b) bekezdését jelölte meg. Ez a jogszabályhely írja elő az adatigénylő részére azt az alapvető követelményt, hogy ha nem adja meg a nevét és az elérhetőségét, akkor az adott szerv nem köteles eleget tenni az igénylésének.

5. sz. ábra

A nemzetbiztonsági szolgálatokhoz benyújtott adatigénylések összesített száma, éves bontásban



Forrás: saját szerkesztés.

Általánosságban levonható az a következtetés, hogy a közérdekű adatigénylések száma az ország lakosságának számához viszonyítva rendkívül alacsony, ahol mégis nagyobb számú megkeresés érkezik, ott pedig az igénylés megtagadásának aránya rendkívül magas.

Tehát a dolgozatban tárgyalt rendvédelmi szervek irányába közérdekű adatigénylések benyújtása, az információkhoz való hozzájutás céljából,– az előzetes hipotézisemet alátámasztva, – nem bevett eljárás a magyar társadalomban.

VI. De lege ferenda javaslatok

A dolgozatban bemutatott problémakörök kapcsán a következő de lege ferenda javaslatokkal az állampolgárok magánszférájának védelme, a titkos információgyűjtés törvényességének nagyobb fokú biztosítása, valamint a közadatokhoz való hozzáférés arányának növelése is megoldható lenne.

1. A jogosulatlan titkos információgyűjtés szabályozása kapcsán

A Btk. 307. §-ban szabályozott jogosulatlan titkos információgyűjtés bűncselekménye kapcsán nem csak a külső, hanem a belső engedélyezésen alapú hatásköri túllépést is be kellene vonni a tényállási elemek közé. Jelenleg a belső engedélyen alapú információgyűjtés szabálytalan kivitelezése a nemzetbiztonsági szervezetek belső ellenőrzésének hatáskörébe tartozik, amely így kevésbé átláthatóbb, mint a bírói úton történő számonkérés eshetősége, valamint az állampolgárok részére sem nem nyújt megfelelő kontrollehetőséget sem. Mivel a hatályos büntetőjogunk tiltja a kiterjesztő értelmezést, ezért célszerű lenne a Btk. 307. § alapján büntetendő jogosulatlan információgyűjtés tárgykörébe foglalni a belső engedélyen alapuló információgyűjtő tevékenységek engedélyi túllépésének szankcionálását is.

2. Az információszabadság hatékonyságának növelése érdekében

A közérdekű és közérdekből nyilvános adatokhoz való hozzáférés lehetőségét úgy lehetne bővíteni, hogy létre kellene hozni egy kifejezetten a közzétételek megfelelősségét vizsgáló, valamint az igénylésekkel foglalkozó hivatalt, amelyen keresztül történne mind az igénylés, mind a válaszok továbbítása az adatigénylőhöz. Ez a megoldás többlet adatvédelmi hátteret is adna, hiszen egy köztes szervezetnek kellene kezelnie a kérelmező adatait, így az a szervezet, akihez benyújtja, nem értesülne az igénylő személyazonosságáról. Ugyanezen szervezet lenne jogosult az adatigénylések megtagadása miatt indított perek esetében felperesi képviseletre, így jóval professzionálisabb, felkészültebb jogi segítségnyújtásban részesülnének a kérelmezők is.

VII. Zárszó

A nemzetbiztonsági szervek tevékenységére, az elsődleges feladataikból eredően, ami a kormányzati hírigények kiszolgálása, a politikai életben, irányvonalakban történő változások is hatással vannak. Az olyan stratégia, amely az állampolgárok biztonságérzetére helyezi a hangsúlyt, az állami szervek számára is több lehetőséget nyújt az emberek magánszférájába történő beavatkozás kivitelezésére, akár látszólagos egyetértéssel is. Az adatvédelem, mint a magánszféra és az információs önrendelkezési jog szabályozási kerete, csak iránymutatásul tud szolgálni a titkos információgyűjtések során, hiszen, mint ahogy rámutattam, azok a garanciális keretek, amelyek jellemzőek az állampolgár-

ok és az általános adatkezelők, adatfeldolgozók közötti kapcsolatban, a nemzetbiztonsági szervek kapcsán nem tudnak érvényesülni. Az Alkotmánybíróság az alapjogkorlátozás egyetlen olyan jogorvoslati szerve, amely a tevékenysége során határt tudna szabni a nemzetbiztonsági szervek számára, a korlátozás szükségtelenségének vagy aránytalanságának megállapításával, azonban, mint láthattuk, a magyar jogértelmezés sokkal megengedőbb az európai standardokhoz képest.

Ahhoz, hogy a nemzetbiztonsági szervek az újabb és újabb elektronikus rendszereket titkos információgyűjtésre tudják használni, egyre inkább egy jelenleg kevésbé szabályozott, vagy egyenesen szabályozatlan jogszabályi környezetben lesznek kénytelenek mozogni. Ezért fontos, hogy a fő irányvonal a meglévő törvényi keretek betartása, a nemzetbiztonsági érdek szűken történő értelmezése és a titkos információgyűjtő műveletek során, a legenyhébb magánszférába történő beavatkozó eszköz választása legyen, hiszen így az állampolgárok bizalma töretlen marad az állami szervek működésével és tevékenységeivel kapcsolatban.

ENIKŐ SZECSKÓ

THE PREVALENCE OF THE INFORMATION FREEDOMS IN THE FIELD OF LAW ENFORCEMENT

(Summary)

The aim of my essay is to study the appearance of data protection and freedom of information in the case of the Hungarian Police and national security services.

After having presented the theoretical background of data protection, I furthermore analyze the national security services' practice regarding measures of secret information gathering from the point of view of constitutional guarantees and the violation of privacy. In this part, I shall point to a number of theoretical alternatives and options that do not fully meet the requirement of the constitutional necessity-proportionality test.

In the second part of my paper, I examine the enforcement of freedom of information through the comparison of the Hungarian Police and national security services. The twenty-eight requests for data of public interest filed by me served as the basis of my empirical research, which I have examined on the formal level and on the level of content. The results of this examination confirmed my research hypothesis, Hungarian does not have a great tradition in wanting to have access to data of public interest.

As the result of my review, I make two de lege ferenda suggestions in my paper. The first is an amendment proposal idea of the effective Criminal Code, inspired by the measures of secret information gathering. The second suggestion is based on a foreign example and its intent is to increase the awareness regarding freedom of information to resolve the apparent civic indifference presented in my paper.